

CLAIMS

What is claimed is:

- 1 1. A method for managing a network boot of a client computer, the method comprising:
2 storing a list of trusted boot program servers in an interface service card coupled to a
3 client computer on a network, the interface service card also being coupled to a hyper-secure
4 remote service network;
5 broadcasting a request for a boot program from the client computer to a network of boot
6 program servers;
7 receiving a response to the request for the boot program at the client computer, the
8 response being from a responding boot program server on the network of boot program servers;
9 comparing an identity of the responding boot program server with the list of trusted boot
10 program servers; and
11 upon verifying that the responding boot program server is on the list of trusted boot
12 program servers, requesting and downloading onto the client computer a boot program from the
13 responding boot program server.
- 1 2. The method of claim 1, further comprising:
2 upon determining that the responding boot program server is not on the list of trusted
3 boot program servers, blocking the requesting of the boot program from the responding boot
4 program server.
- 1 3. The method of claim 2, further comprising:
2 upon determining that the responding boot program server is not on the list of trusted
3 boot program servers, generating an alert to a designated administrator of a presence of an
4 unauthorized boot program server on the network of boot program servers.
- 1 4. The method of claim 1, wherein the designated administrator communicates with the
2 client computer via the hyper-secure remote service network.

1 5. The method of claim 4, wherein the comparing step is performed by configuring the
2 client computer to perform Layer 3 packet filtering to identify Pre-boot Execution
3 Environment/Bootstrap Protocol (PXE/BootP) traffic, wherein Layer 3 is a network layer of the
4 seven layers of the Open System Interconnection (OSI) model.

1 6. The method of claim 1, further comprising:
2 upon determining that the responding boot program server is not on the list of trusted
3 boot program servers, downloading a boot program from a known trusted boot server in a secure
4 local area network (LAN).

1 7. The method of claim 1, wherein the client computer is a server blade.

1 8. The method of claim 7, further comprising:
2 managing different types of boot program servers available to the server blade by
3 maintaining, in an information technology services organization logically oriented between the
4 different types of boot program servers and the server blade, a permission list of boot program
5 servers authorized for each server blade in a server blade chassis.

1 9. A system for managing a network boot of a client computer, the system comprising:
2 means for storing a list of trusted boot program servers in an interface service card
3 coupled to a client computer on a network, the interface service card also being coupled to a
4 hyper-secure remote service network;
5 means for broadcasting a request for a boot program from the client computer to a
6 network of boot program servers;
7 means for receiving a response to the request for the boot program at the client computer,
8 the response being from a responding boot program server on the network of boot program
9 servers;
10 means for comparing an identity of the responding boot program server with the list of
11 trusted boot program servers; and

12 means for, upon verifying that the responding boot program server is on the list of trusted
13 boot program servers, requesting and downloading onto the client computer a boot program from
14 the responding boot program server.

1 10. The system of claim 9, further comprising:

2 means for, upon determining that the responding boot program server is not on the list of
3 trusted boot program servers, blocking the requesting of the boot program from the responding
4 boot program server.

1 11. The system of claim 10, further comprising:

2 means for, upon determining that the responding boot program server is not on the list of
3 trusted boot program servers, generating an alert to a designated administrator of a presence of
4 an unauthorized boot program server on the network of boot program servers.

1 12. The system of claim 9, wherein the designated administrator communicates with the
2 client computer via the hyper-secure remote service network.

1 13. The system of claim 12, wherein the means for comparing is performed by means for
2 configuring the client computer to perform Layer 3 packet filtering to identify Pre-boot
3 Execution Environment/Bootstrap Protocol (PXE/BootP) traffic, wherein Layer 3 is a network
4 layer of the seven layers of the Open System Interconnection (OSI) model.

1 14. The system of claim 9, further comprising:

2 means for, upon determining that the responding boot program server is not on the list of
3 trusted boot program servers, downloading a boot program from a known trusted boot server in a
4 secure local area network (LAN).

1 15. The system of claim 9, wherein the client computer is a server blade.

1 16. The system of claim 15, further comprising:

2 means for managing different types of boot program servers available to the server blade
3 by maintaining, in an information technology services organization logically oriented between
4 the different types of boot program servers and the server blade, a permission list of boot
5 program servers authorized for each server blade in a server blade chassis.

1 17. A computer program product, residing on a computer usable medium, for managing a
2 network boot of a client computer, the computer program product comprising:

3 program code for storing a list of trusted boot program servers in an interface service card
4 coupled to a client computer, the interface service card also being coupled to a hyper-secure
5 remote service network;

6 program code for broadcasting a request for a boot program from the client computer to a
7 network of boot program servers;

8 program code for receiving a response to the request for the boot program at the client
9 computer, the response being from a responding boot program server on the network of boot
10 program servers;

11 program code for comparing an identity of the responding boot program server with the
12 list of trusted boot program servers; and

13 program code for, upon verifying that the responding boot program server is on the list of
14 trusted boot program servers, requesting and downloading onto the client computer a boot
15 program from the responding boot program server.

1 18. The computer program product of claim 17, further comprising:

2 program code for, upon determining that the responding boot program server is not on the
3 list of trusted boot program servers, blocking the requesting of the boot program from the
4 responding boot program server.

1 19. The computer program product of claim 18, further comprising:

2 program code for, upon determining that the responding boot program server is not on the
3 list of trusted boot program servers, generating an alert to a designated administrator of a
4 presence of an unauthorized boot program server on the network of boot program servers.

1 20. The computer program product of claim 17, wherein the designated administrator
2 communicates with the client computer via the hyper-secure remote service network.

1 21. The computer program product of claim 20, wherein the program code for comparing is
2 performed by program code for configuring the client computer to perform Layer 3 packet
3 filtering to identify Pre-boot Execution Environment/Bootstrap Protocol (PXE/BootP) traffic,
4 wherein Layer 3 is a network layer of the seven layers of the Open System Interconnection (OSI)
5 model.

1 22. The computer program product of claim 17, further comprising:

2 program code for, upon determining that the responding boot program server is not on the
3 list of trusted boot program servers, downloading a boot program from a known trusted boot
4 server in a secure local area network (LAN).

6 23. The computer program product of claim 17, wherein the client computer is a server blade.

1 24. The computer program product of claim 23, further comprising:

2 program code for managing different types of boot program servers available to the
3 server blade by maintaining, in an information technology services organization logically
4 oriented between the different types of boot program servers and the server blade, a permission
5 list of boot program servers authorized for each server blade in a server blade chassis.